

What is claimed is:

1. A computer-implemented system for facilitating the issuance and exchange of a stable cryptocurrency collateralized by government-issued debt, the system comprising:

a management platform in communication with a transaction validation and recording network including a plurality of distributed nodes configured to store blockchain data structures, the management platform including:

a memory configured to store computer program instructions relating to at least a smart contract module and an identity (ID) and risk score module; and

one or more physical computer processors configured by the computer program instructions to implement at least the smart contract module and the ID and risk score module, the computer program instructions including instructions for:

establishing a first digital wallet associated with a first user and a second digital wallet associated with a second user;

determining, based upon user parameters and financial information associated with the first user, first wallet metadata for the first digital wallet wherein the first wallet metadata includes at least one of a first risk score and a first ID verification classification;

storing the first wallet metadata on a blockchain within the transaction validation and recording network;

enabling, using a restricted use key generated based upon granularity information associated with the first digital wallet, the second digital wallet to access the first wallet metadata stored on the blockchain at a level of granularity determined by the granularity information;

receiving a first transaction request involving at least the first digital wallet and the second digital wallet; and

responding to the first transaction request based upon at least one of: (i) a comparison of the first wallet metadata to transaction rules associated with the second digital wallet, and (ii) user input provided by the second user upon consideration of the first wallet metadata at the level of granularity determined by the granularity information.

2. The system of claim 1, wherein the instructions for evaluating further include comparing second wallet metadata associated with the second digital wallet to additional transaction rules associated with the first digital wallet.
3. The system of claim 1, wherein the instructions further include instructions for facilitating completion of a first transaction corresponding to the first transaction request and recording the first transaction in the blockchain.
4. The system of claim 1, wherein the instructions further include instructions for:
rejecting, based upon the evaluating, the first transaction request;
recording a rejection of the first transaction request in the blockchain.
5. The system of claim 1, wherein the first transaction request corresponds to a transfer request and wherein the instructions further include instructions for transferring, based upon the evaluating, a specified number of tokens of the stable cryptocurrency from the first digital wallet to the second digital wallet.
6. The system of claim 1, wherein the memory is further configured to store instructions for a know your customer (KYC) module, the instructions for the KYC module including instructions for:
determining a first know your customer (KYC) score based upon at least some of the user parameters and financial information associated with the first user; and
creating a first public address and corresponding private key for the first digital wallet based at least in part upon the first KYC score.
7. The system of claim 6, wherein the instructions for the KYC module further include instructions for performing a KYC check of the first user based upon rules applicable to a jurisdiction in which the first user is located wherein such rules include at least one of residence-based KYC laws and anti-money laundering (AML) laws.
8. The system of claim 1, wherein the instructions further include instruction for:
receiving a second transaction request involving at least the first digital wallet;
evaluating the second transaction request based upon additional transaction rules associated with the first digital wallet.

9. The system of claim 8, wherein the second transaction request corresponds to a redemption request and wherein the instructions further include instructions for redeeming, subsequent to the evaluating the second transaction request, a specified number of tokens of the stable cryptocurrency from the first digital wallet.

10. The system of claim 4, wherein the instructions further include instructions for adjusting the first risk score based on any of: (i) rejection of the first transaction request, (ii) acceptance of the first transaction request, and (iii) a completed transfer of a specified number of tokens of the stable cryptocurrency from the first digital wallet to the second digital wallet.

11. The system of claim 1, wherein the memory is further configured to store instructions for a know your customer (KYC) module, the instructions for the KYC module including instructions for determining a first know your customer (KYC) score based upon at least some of the personal and financial information associated with the first user wherein the first set of rules are further premised at least in part on the first KYC score.

12. The system of claim 1, wherein the memory is further configured to store instructions for an artificial intelligence (AI) engine, the instructions for the AI engine including:

determining a net amount of the government-issued currency received, at an account associated with an operator of the system, from users of the system;

determining, based upon the net amount of the government-issued currency received, a plurality of new tokens of the stable cryptocurrency to be created;

determining an amount of the government-issued debt required to be purchased to collateralize the plurality new tokens of the stable cryptocurrency;

creating, and issuing to digital wallets associated with the users of the system, the plurality of new tokens of the stable cryptocurrency.

13. The system of claim 1, wherein the memory is further configured to store instructions for an artificial intelligence (AI) engine, the instructions for the AI engine including:

determining a net amount of the government-issued currency withdrawn, at an account associated with an operator of the system, by users of the system;

determining, based upon the net amount of the government-issued currency withdrawn, a plurality of existing tokens of the stable cryptocurrency to be destroyed;

determining an amount of the government-issued debt required to be sold in connection with destruction of the plurality of existing tokens of the stable cryptocurrency;
destroying the plurality of existing tokens of the stable cryptocurrency.

14. The system of claim 1, wherein the instructions further include instructions for periodically recalculating the first risk score, the user parameters used in recalculating the first risk score relating to a source of the government-issued currency provided by the first user, a source of wealth of the first user and a verification of an address of the first user.

15. The system of claim 1, wherein the instructions further include instructions for periodically recalculating the first risk score, the financial information used in recalculating the first risk score including information relating to bank account verification, credit card verification, and assets verification.

16. The system of claim 1, wherein the instructions further include instructions for recalculating the first risk score in response to at least one of (i) a change in any of the user parameters, (ii) completion or attempt of a transaction involving the first digital wallet, (iii) counter party risk information including a second risk score and second ID verification classification for the second digital wallet.

17. The system of claim 1, wherein the instructions further include instructions for:
determining, based upon at least one of the first risk score and the first ID verification classification, that the first digital wallet is eligible to receive a plurality of tokens of the stable cryptocurrency from the second digital wallet or in exchange for government-issued currency provided by the first user;
transferring the plurality of tokens from a treasury wallet to the first digital wallet.

18. The system of claim 1, wherein the instructions include instructions for adjusting the first risk score based upon parameters of a transaction occurring between the first digital wallet and a second digital wallet.

19. The system of claim 1, wherein the second digital wallet is configured with a set of rules relating to transaction eligibility and is further configured to determine whether the first risk score and the first ID verification classification comport with the set of rules.

20. The system of claim 1, wherein information relating to at least one of the first risk score and the first ID verification classification is provided for review by the second user at the level of granularity determined by the granularity information used in generating the restricted use key.

21. The system of claim 1, wherein the instructions include instructions for adjusting the first risk score and a second risk score associated with the second digital wallet based upon transactions occurring between the first digital wallet and the second digital wallet.

22. The system of claim 1, wherein the instructions include instructions for adjusting the first risk score and a second risk score associated with the second digital wallet based upon a rejection of a transaction proposed between the first digital wallet and the second digital wallet.

23. A method for facilitating the issuance and exchange of a stable cryptocurrency collateralized by government-issued debt, the method being implemented by a management platform in communication with a transaction validation and recording network including a plurality of distributed nodes, the management platform including a memory configured to store computer program instructions relating to at least a smart contract module and an ID and risk score module, the management platform further including one or more physical computer processors configured by the computer program instructions to implement at least the smart contract module and the ID and risk score module, the method comprising:

establishing a first digital wallet associated with a first user and a second digital wallet associated with a second user;

determining, based upon user parameters and financial information associated with the first user, first wallet metadata for the first digital wallet wherein the first wallet metadata includes at least one of a first risk score and a first ID verification classification;

storing the first wallet metadata on a blockchain within the transaction validation and recording network;

enabling, using a restricted use key generated based upon granularity information associated with the first digital wallet, the second digital wallet to access the first wallet metadata stored on the blockchain at a level of granularity determined by the granularity information;

receiving a first transaction request involving at least the first digital wallet and the second digital wallet; and

responding to the first transaction request based upon at least one of: (i) a comparison of the first wallet metadata to transaction rules associated with the second digital wallet, and (ii) user input provided by the second user upon consideration of the first wallet metadata at the level of granularity determined by the granularity information.

24. A method for facilitating the exchange of a stable cryptocurrency collateralized by government-issued debt, the method being implemented by a management platform in communication with a transaction validation and recording network including a plurality of distributed nodes configured to store blockchain data structures, the management platform including a memory configured to store computer program instructions relating to at least an ID and risk score module, the management platform further including one or more physical computer processors configured by the computer program instructions to implement at least the ID and risk score module, the method comprising:

receiving, through a first wallet interface of a first digital wallet, first granularity parameters of a first restricted use key;

generating the first restricted use key using the first digital wallet;

providing the first restricted use key to an owner of a second digital wallet;

receiving a second restricted use key wherein the second restricted use key is generated by the second digital wallet based upon second granularity parameters received through a second wallet interface associated with the second digital wallet;

accessing, using the second restricted use key, information from a blockchain wallet wherein the information relates to one or more of an ID classification and risk score of the owner of the second digital wallet at a level of detail determined by the second granularity parameters; and

receiving, through the first wallet interface, an indication to proceed with a transaction between the first digital wallet and the second digital wallet.